CLAIMS

I claim:

1. A method of securely conveying a data product, the method comprising the steps of:

establishing an authorization key that defines (i) verification information indicative of at least one authorized entity and (ii) a cryptographic key to the data product;

encrypting the authorization key, thereby producing an encrypted authorization key that can be decrypted using a decryption key; and

providing the encrypted authorization key to a system that (i) has access to the decryption key and can therefore decrypt the encrypted authorization key and (ii) is programmed to decrypt the authorization key and to use the verification information to validate use of the data product.

2. The method of claim 1, further comprising the steps of:

receiving the encrypted authorization key;

using the decryption key to decrypt the encrypted authorization key, and thereby uncovering the verification information and the cryptographic key to the data product; and

using the verification information to validate use of the data product.

3. The method of claim 2, wherein using the verification information to validate use of the data product comprises comparing at least a portion of the verification information to predetermined information associated with the system, to determine whether the system is authorized to use the data product.

4. The method of claim 3, wherein the predetermined information associated with the system comprises a system ID.

5. The method of claim 1, wherein providing the encrypted authorization key to the system comprises sending the encrypted authorization key to the system via a wireless communications network.

6. The method of claim 1, wherein providing the encrypted authorization key to the system comprises recording the encrypted authorization key on a data storage medium and then providing the data storage medium to the system.

7. The method of claim 6, further comprising the steps of:

the system reading the encrypted authorization key from the data storage medium;

the system using the decryption key to decrypt the encrypted authorization key and thereby uncovering the verification information and the cryptographic key to the data product; and

the system using the verification information to validate use of the data product.

8. The method of claim 7, wherein using the verification information to validate use of the data product comprises comparing at least a portion of the verification information to predetermined information associated with the data storage medium, to determine whether the data storage medium is authorized to store the data product.

9. The method of claim 8, wherein the predetermined information associated with the data storage medium comprises a data storage medium ID.

10. The method of claim 1, wherein the data product comprises a database of geographic information.

11. A method of securely conveying data, the method comprising the steps of:

assembling a set of authorization parameters associated with the data;

computing a first checksum of the set of authorization parameters;

generating a first cryptographic key substantially randomly;

using the first cryptographic key to symmetrically encrypt the set of authorization parameters, so as to produce an encrypted set of authorization parameters;

encrypting a combination of the first cryptographic key and the first checksum, so as to produce a header value that can be decrypted using a second cryptographic key; and

providing the header value, together with the data, for access by a receiving end.

12. The method of claim 11, further comprising the following steps performed at the receiving end:

using the second cryptographic key to decrypt the header value, so as to produce an decrypted header value;

retrieving the first cryptographic key and first checksum from the decrypted header value;

using the first cryptographic key to decrypt the encrypted set of authorization parameters;

computing a second checksum of the set of authorization parameters;

comparing the second checksum with the first checksum, and refusing to access the data if the second checksum does not match the first checksum; and

using the set of authorization parameters to verify authorization to access the data.

13. The method of claim 12, further comprising encrypting the data before providing the data and header value for access by the receiving end.

14. A method of securely conveying data, the method comprising the steps of:

assembling an authorization key that includes verification information indicative of a data storage medium on which the data is authorized to be stored; and

encrypting the authorization key and the data, thereby producing an encrypted authorization key and encrypted data;

storing the encrypted authorization key and encrypted data on a given data storage medium; and

thereafter providing the given data storage medium to a system that is programmed to decrypt the authorization key and to determine, by reference to the verification information whether the given storage medium is the data storage medium on which the data is authorized to be stored.

15. The method of claim 14, further comprising the system decrypting the encrypted data only if the verification information indicates that the given storage medium is the data storage medium on which the date is authorized to be stored.

16. A method of securely communicating a data product, while allowing the data product to be used in connection with at least one authorized entity, the at least one authorized entity having an associated identification code, the method comprising:

symmetrically encrypting at least a portion of the data product using a first cryptographic key, thereby producing an encrypted portion of the data product that can be symmetrically decrypted using the first cryptographic key;

establishing an authorization key including verification information;

computing a first value as a first function of input parameters including (i) the identification code and (ii) a second value;

combining the first value with the first cryptographic key to produce a third value;

adding the third value to the authorization key;

thereafter using the first value as a second cryptographic key to symmetrically encrypt the authorization key, so as to produce an encrypted authorization key that can be decrypted using the first value;

encrypting at least the second value to produce an encrypted value that can be decrypted using a third cryptographic key; and

providing to a receiving-end at least (i) the encrypted value, (ii) the encrypted authorization key, and (iii) the encrypted portion of the data product,

whereby, if the receiving end has access to the third cryptographic key and the input parameters, the receiving end may be able to uncover the first authorization key and the cryptographic key and may therefore be able to access the verification information and decrypt the encrypted portion of the data product.

17. The method of claim 16, wherein the data product comprises geographical information, the authorized entity comprises a navigation system, and the identification code comprises a navigation system ID.

18. The method of claim 16, wherein the data product comprises geographical information, the authorized entity comprises a data storage device, and the identification code comprises a storage device ID.

19. The method of claim 16, wherein the first function comprises a hash function.

20. The method of claim 19, wherein the input parameters further include a predetermined segment of the encrypted portion of the data product.

21. The method of claim 16, wherein combining the first value with the first cryptographic key to produce a third value comprises computing an XOR sum of the first value and the first cryptographic key.

22. The method of claim 16, wherein encrypting at least the second value to produce an encrypted value that can be decrypted with a third cryptographic key comprises:

combining the second value with a checksum of the authorization key; and

using a public key encryption algorithm to encrypt the second value

23. The method of claim 16, further comprising the following steps:

receiving at the receiving-end (i) the encrypted value, (ii) the encrypted authorization key, and (iii) the encrypted portion of the data product,

using the third cryptographic key to decrypt the encrypted value

computing the first value as the first function of the input parameters;

using the first value as the second cryptographic key to symmetrically decrypt the encrypted authorization key;

extracting the third value from the authorization key;

using the third value and the first value to generate the first cryptographic key; and

using the first cryptographic key to symmetrically decrypt the encrypted portion of the data product.

24. Th method of claim 23, further comprising, at the receiving-end, verifying the checksum of the authorization key.

25. The method of claim 23, wherein using the third value and the first value to generate the first cryptographic key comprises computing an XOR sum of the third value and the first value.

26. The method of claim 23, further comprising the step of validating use of the data product by reference to the verification information.

27. A method of securing a data product against unauthorized use, while allowing the data product to be used in connection with at least one authorized entity, the at least one authorized entity having an associated identification code, the method comprising:

symmetrically encrypting at least a portion of the data product using a first cryptographic key, thereby producing an encrypted portion of the data product that can be symmetrically decrypted using the first cryptographic key;

establishing an authorization key including verification information;

computing a first value as a first function of input parameters including (i) the identification code and (ii) a second value;

combining the first value with the first cryptographic key to produce a third value;

adding the third value to the authorization key;

thereafter using the first value as a second cryptographic key to symmetrically encrypt the authorization key, so as to produce an encrypted authorization key that can be decrypted using the first value; and

encrypting at least the second value to produce an encrypted value that can be decrypted using a third cryptographic key.

28. The method of claim 27, further comprising randomly generating the first cryptographic key.

29. The method of claim 27, wherein the portion of the data product comprises the entire database.

30. The method of claim 27, wherein the portion of the data product comprises information required to understand contents of the data product.

31. The method of claim 30, wherein the information required to understand contents of the data product is selected from the group consisting of (i) database decompression information and (ii) pointers.

32. The method of claim 27, wherein the data product comprises geographic information.

33. The method of claim 27, wherein the data product comprises geographic information, the authorized entity comprises a navigation system, and the identification code comprises a navigation system ID.

34. The method of claim 27, wherein the data product comprises geographic information, the authorized entity comprises a data storage device, and the identification code comprises a storage device ID.

35. The method of claim 27, wherein the first function comprises a hash function.

36. The method of claim 27, wherein the input parameters further include a predetermined segment of the encrypted portion of the data product.

37. The method of claim 27, wherein combining the first value with the first cryptographic key to produce a third value comprises computing an XOR sum of the first value and the first cryptographic key.

38. The method of claim 27, wherein encrypting at least the second value to produce an encrypted value that can be decrypted with a third cryptographic key comprises:

combining the second value with a checksum of the authorization key; and

using a public key encryption algorithm to encrypt the second value

39. A system for securing a data product against unauthorized use, while allowing the data product to be used in connection with at least one authorized entity, the system comprising:

a processor;

a data storage medium; and

a set of machine language instructions stored in the data storage medium and executable by the processor to carry out the method steps of claim 27.